

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Doug Rollins

Application No.: 09/993,495

Confirmation No.: 8165

Filed: November 27, 2001

Art Unit: 2437

For: METHOD AND APPARATUS FOR WEP KEY
MANAGEMENT AND PROPAGATION IN A
WIRELESS SYSTEM

Examiner: S. Gelagay

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with 37 C.F.R. 41.37(a), this brief is filed within one month of the receipt of the Notice of Panel Decision from Pre-Appeal Review mailed June 22, 2010.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

- | | |
|------|-----------------------------------------------|
| I. | Real Party In Interest |
| II | Related Appeals and Interferences |
| III. | Status of Claims |
| IV. | Status of Amendments |
| V. | Summary of Claimed Subject Matter |
| VI. | Grounds of Rejection to be Reviewed on Appeal |

VII.	Argument
VIII.	Conclusion
Appendix A.	Claims Appendix
Appendix B.	Evidence Appendix (none)
Appendix C.	Related Proceedings Appendix (none)

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is: Micron Technology, Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 25 claims pending in application. The application contains claims 1-12 and 14-26, which were finally rejected. This is an appeal from the final rejection of claims 1-12 and 14-26.

B. Current Status of Claims

1. Claims canceled: 13
2. Claims withdrawn from consideration but not canceled: N/A
3. Claims pending: 1-12 and 14-26.
4. Claims allowed: None.
5. Claims rejected: 1-12 and 14-26.

C. Claims On Appeal

The claims on appeal are claims 1-12 and 14-26.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the Final Rejection mailed September 11, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention is directed to encryption key management in a wireless system. Encryption key updates are performed using a wired device on a wired network to which wireless network communications devices are physically connected. (Abstract, ¶ [0013])¹

As discussed in the specification, “when an encryption key is to be updated, [a] wireless network communications device card is removed from [a] wireless station and inserted into a card tray connected to a wired portion of the network. A management station randomly generates a new encryption key and propagates it to all access points and to one or more card trays. The card trays may be conventional personal computer card trays, e.g. PCMCIA or other PC card trays. Once the encryption key is updated at each access point and the one or more PC card trays and the encryption key in each of the wireless network communications devices is updated. The wireless network communications devices having updated encryption keys may then be removed from the card trays and reinserted into the wireless stations.” ([0013]). An example embodiment is reproduced below in FIG. 4.

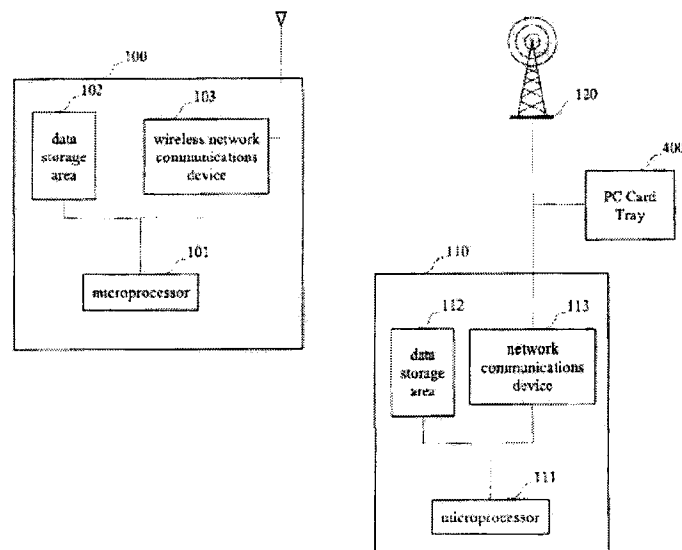


FIG. 4, present application

¹ Reference herein is made to paragraph numbers of the present application’s specification as published in U.S. Patent Application Publication No. 2003/0099362 A1.

The FIG. 4 system comprises a wireless network provided by access point 120 which is connected to a wired network, including a wired management station 110 and an exemplary card tray 400. ([0020]). Wireless station 100 (*i.e.* a laptop) which connects to access point 120 has a removable wireless network communications device 103 installed therein. ([0020]).

When an encryption key update is required, “[c]ard tray 400 has a plurality of slots each of which can receive an inserted wireless network communications device 103 ... When wireless network communications device 103 is inserted into a slot of PC card tray 400, and the PC card tray 400 receives a new encryption key, PC card tray 400 accesses the encryption key stored in wireless communications device 103, erases the old encryption key and stores the updated encryption key... [I]f a PC card tray 400 has already received a new encryption key when wireless communications device 103 is inserted, PC card tray 400 can then access the encryption key stored in wireless communications device 103, erase the old encryption key and store the updated encryption key.” ([0020]).

“By allowing wireless communications device 103 to be updated by placing it in PC card tray 400 , greater network security and reliability is achieved. First, since the encryption key is not written down and entered manually, there is no chance of the network administrator making an error while typing in the new encryption key. Second, since not even the network administrator knows what the encryption key is, the only way to obtain the encryption key is by gaining physical access to the network. Third, the network administrator does not have to physically access each wireless station 100 . A technician, or even the user, can remove network communications device 103 from wireless station 100 and insert it into PC card tray 400 . There can be many PC card trays connected to the wired network and placed at convenient locations so that the inconvenience is minimized.” ([0029]).

Turning now to the claims, claim 1 recites “a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network” ([0013]. [0020]) The method requires “physically separating from said wireless station [*i.e.*, 100 in FIG. 4] a network communications device [*i.e.*, 103 in FIG. 4].” ([0020]). The network

communications device is “physically connect[ed] ... to an encryption key updating device [*i.e.*, card tray 400 in FIG. 4] which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator [*i.e.* wired management station 110 in FIG. 4] for providing a new encryption key to said updating device.” ([0013], [0020]). The updating device “replac[es] an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network.” ([0013],[0020]). Once done, the method includes “physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and accessing said new encryption key on said network communications device during an encrypted communication.” ([0013],[0020]).

Independent claim 8 recites a network comprising 1) “a wired station [*i.e.*, wired management station 110 in FIG. 4] connected to a wired network, said wired station comprising: an encryption key generator for generating an encryption key; a network communications device [*i.e.*, 113 in FIG. 4] for transmitting said encryption key over said wired network” ([0013], [0020]); 2) a “wired encryption key updating device [*i.e.* card tray 400 in FIG. 4] connected to said wired network” ([0013], [0020]); and 3) a “wireless station [*i.e.*, 100 in FIG. 4] configured to be wirelessly connected to said network and to communicate with said wired network through communications encrypted with an encryption key.” ([0013], [0020]). The wireless station comprises “a wireless network communications device [*i.e.*, 103 in FIG. 4] containing said encryption key, said wireless station configured to access said encryption key on said wireless network communications device during said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to said wired encryption key updating device wired to said network to receive, store, and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device.” ([0013],[0020]).

Independent claim 15 recites a wireless network station, *i.e.*, station 100 in FIG. 4. That station has a “wireless network communications device [*i.e.*, 103 in FIG. 4] for conducting wireless communications with a wired network, said wireless network communications device being

physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable [*i.e.* via card tray 400 in FIG. 4] to a wired network to receive, store, and use a new encryption key, said wireless station configured to access an encryption key on said wireless network communications device during a wireless communication.” ([0013],[0020]).

Similarly, independent claim 17 recites a wireless network communications device, *i.e.*, 103 in FIG. 4. The device includes “a removable wireless communications network card adapted to be physically connected to and disconnected from a wireless station card interface [*i.e.*, on station 100 in FIG. 4]; and a storage area on said network card which stores an updateable encryption key for use by a wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface [*i.e.* card tray 400 in FIG. 4] which supplies a new encryption key, said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication.” ([0013],[0020]).

Lastly, claim 20 recites an encryption key programming system which includes “an encryption key generator”, *i.e.*, wired management station 110 in FIG. 4, “connected to a wired network,” and “a programming device connected to said wired network [*i.e.* card tray 400 in FIG. 4] for receiving over a wire connection a new encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device [*i.e.*, 103 in FIG. 4] containing an updatable encryption key and storing said received encryption key in said wireless network communications device, said new encryption key on said wireless network communications device being accessible by a wireless network device during encrypted communications.” ([0013],[0020]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1, 6-8, 14-20 and 26 are properly rejected as being unpatentable over U.S. Patent 7,024,553 to Morimoto in view of U.S. Patent 6,055,314 to Spies, et al. (“Spies”).

B. Whether claims 2-3, 9-10, and 21-23 are properly rejected as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 4,369,332 to Campbell, Jr. (“Campbell”).

C. Whether claims 4-5, 11-12 and 24-25 are properly rejected as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 6,226,750 to Trieger (“Trieger”).

VII. ARGUMENT

- A. The § 103(a) rejection of claims 1, 6-8, 14-20 and 26 must be withdrawn because the Morimoto and Spies combination is improper, and also fails to disclose, teach or suggest each and every element of the claims.

Appellant respectfully requests this Board to reverse the Examiner’s pending rejection because, as shown below, it has no basis in fact or in law. Novelty is not in doubt—the examiner was unable to find the claimed invention in any single reference. In fact, the Examiner only alleges to find the claimed invention in two references, which as will be shown below, cannot be combined, and even then fail to disclose, teach or suggest each and every element of the claims. For these reasons discussed in more detail below, Appellant respectfully urges the Board to reverse the pending rejection and allow the claims.

1. *Morimoto explicitly teaches away from physical attachment of a separated network communications device to a wired encryption key updating device; further, combination with Spies would frustrate Morimoto’s purpose*

MPEP § 2143.03(VI) states that “[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention.” Accordingly, where cited art teaches away from a claimed feature, the cited art cannot be used in an obviousness rejection. Moreover, “the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose.” MPEP § 2143.01.

Claim 1 is directed to a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, and recites “physically separating from said wireless station a network communications device; physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and accessing said new encryption key on said network communications device during an encrypted communication.”

In the present case, Appellant submits that the Office’s characterizations of the teachings of paras. [0021-0026] of the present application’s specification are incorrect and, contrary to what the Office suggests, are *not* consistent with the teachings of Morimoto. Although the present application and Morimoto are both directed to updating encryption keys on a corporate network, their methods are quite different. Morimoto explicitly teaches that “each of STAs 103 memorizes and supervises ... [new] encrypted key[s] delivered from the key management server 101 [wirelessly] through the AP 102 and has communication with the AP using the encrypted key[s].” (Morimoto, col. 7, lns. 62—col. 8, ln. 5). By contrast, the present application teaches updating the encryption key in use on the access point itself, but also updating an encryption key on an updating device (*e.g.*, a PC card tray 400), so that wireless communications devices can be *physically* connected to that device for updating. ([0027]-[0028]). This is especially important because the present application contemplates and distinguishes itself from a Morimoto-type wireless updating system, discussing in [0008] that “[i]f the vendor supplied management application does not [automatically update keys]... then...” the process described in the present application could be used. ([0008]). Morimoto delivers keys to wireless stations directly, *and only*, through its access points. (Morimoto, col. 4, ln. 59—col. 5, ln. 63, FIG. 1).

Considering the discussion above that Morimoto clearly teaches *wireless-only* means of updating WEP keys, Morimoto thus explicitly teaches away from the claimed concept of *physical* attachment of a *separate* network communications device to a *wired* encryption key updating device (which is not an access point) for encryption key distribution, as recited by claim 1.

Furthermore, even if Spies taught “physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device,” which as explained below, it does not, combining the references would be improper. Moreover, combining Morimoto with the teachings of Spies would frustrate the very purpose of Morimoto’s teachings—updating encryption keys *wirelessly*.

Independent claims 8, 15, 17 and 20 recite similar limitations to claim 1, namely “a wireless network communications device containing [an] encryption key, said wireless station configured to access said encryption key on said wireless network communications device during said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to [a] wired encryption key updating device wired to said network to receive, store, and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device,” (Claim 8), “said wireless network communications device being physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable to a wired network to receive, store, and use a new encryption key, said wireless station configured to access an encryption key on said wireless network communications device during a wireless communication,” (Claim 15), “a storage area on said network card which stores an updateable encryption key for use by a wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface which supplies a new encryption key, said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication,” (Claim 17), and “a

programming device connected to said wired network for receiving over a wire connection a new encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device, said new encryption key on said wireless network communications device being accessible by a wireless network device during encrypted communications,” (Claim 20). Appellant submits that the arguments for claim 1 are equally as applicable to claims 8, 15, 17 and 20.

2. *Even if Morimoto and Spies could be combined, Spies cannot cure the admitted deficiencies of Morimoto*

Notwithstanding the argument presented above that the proposed Morimoto and Spies combination is improper, the rationale required to support a conclusion that the claims would have been obvious is that “*all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art.*” MPEP §2143(A) (emphasis added). As discussed in the Pre-Appeal Brief filed December 11, 2009, the Office admits that Morimoto does not teach or suggest at least “physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device.” (Office Action, pg. 3).

Spies, which is directed to a method for secure purchase and delivery of video programs, cannot cure the deficiencies of Morimoto even if the references could be combined. Spies merely teaches distributing *decryption* keys on removable IC cards (e.g., PCMCIA cards) to enable a video player to decode *video content* stored on a DVD or other medium—Spies’ IC cards are not network communications devices, nor do they provide “encryption key[s] used by a wireless station for encrypted communications with a wired portion of the network.” (Spies, Abstract, col. 6, lns. 19-

33). In fact, Spies does not teach or suggest network encryption, much less “physically separating from said wireless station [a] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device,” as recited in claim 1. Spies’ teachings would not permit “accessing said new encryption key on said network communications device during an encrypted communication,” as claimed, because Spies only teaches use of a *decryption* key to decode *specific* encrypted video content. Moreover, the IC card of Spies is not a “separated network communications device.” In fact, separable network communications devices are not taught or suggested anywhere in either Morimoto or Spies.

As noted above, independent claims 8, 15, 17 and 20 recite similar limitations to claim 1 and are believed to be allowable for at least the same reasons as claim 1. Dependent claims 6-7, 14, 16, 18-19 and 26 depend from claims 1, 8, 15, 17 and 20, respectively, and are likewise allowable.

For each of the above discussed reasons, Appellant respectfully submits that the §103 rejection over the proposed Morimoto and Spies combination should be reversed and the claims allowed.

- B. The § 103(a) rejection of claims 2-3, 9-10, and 21-23 must be withdrawn because the Morimoto, Spies and Campbell fails to disclose, teach or suggest each and every element of the claims.

Claims 2-3, 9-10 and 21-23 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Campbell, which is cited by the Office as teaching encryption key regeneration at specific or user-defined intervals, cannot cure the deficiencies of the proposed (defective) Morimoto and Spies combination discussed above. For this reason, Appellant respectfully submits that the §103 rejection over the proposed Morimoto, Spies and Campbell combination should be reversed and the claims allowed.

- C. The § 103(a) rejection of claims 4-5, 11-12 and 24-25 must be withdrawn because the Morimoto, Spies and Triefer fails to disclose, teach or suggest each and every element of the claims.

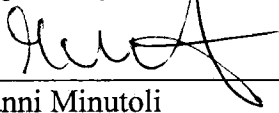
Claims 4-5, 11-12 and 24-25 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Triefer, which is cited by the Office as teaching comparison of newly-generated encryption keys to previous keys to ensure there is no repetition, cannot cure the deficiencies of the proposed (defective) Morimoto and Spies combination discussed above. For this reason, Appellant respectfully submits that the §103 rejection over the proposed Morimoto, Spies and Triefer combination should be reversed and the claims allowed.

VIII. CONCLUSION

For each of the foregoing reasons, Appellant respectfully submits that the claimed invention is patentable over the cited prior art as well as adequately supported and enabled. Reversal of the final grounds of rejection is respectfully solicited.

Dated: July 22, 2010

Respectfully submitted,

By 

Gianni Minutoli

Registration No.: 41,198

Matthew B. Weinstein

Registration No.: 62,202

DICKSTEIN SHAPIRO LLP

1825 Eye Street, NW

Washington, DC 20006-5403

(202) 420-2200

Attorneys for Appellant

APPENDIX A – CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 09/993.495

1. (Previously Presented) A method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:

physically separating from said wireless station a network communications device;

physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device;

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network;

physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and

accessing said new encryption key on said network communications device during an encrypted communication.

2. (Original) A method as in claim 1, wherein said new encryption key is generated at user-defined intervals.

3. (Original) A method as in claim 1, wherein said new encryption key is generated on user-specified days.

4. (Previously Presented) A method as in claim 1, wherein:

said key generator generates a first new encryption key;

compares said new encryption key to the previous k encryption keys used in said network; and

generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

5. (Previously Presented) A method as in claim 4, wherein k is a user-defined number of previously used encryption keys.

6. (Previously Presented) A method as in claim 1, wherein said network communications device is configured on a plug-in card and is physically connected to said network by inserting said network communications device into a card tray at said updating device.

7. (Original) A method as in claim 6, wherein a plurality of network communications devices can be inserted into said card tray simultaneously.

8. (Previously Presented) A network comprising:

a wired station connected to a wired network, said wired station comprising:

an encryption key generator for generating an encryption key;

a network communications device for transmitting said encryption key over said wired network; and

a wired encryption key updating device connected to said wired network;

a wireless station configured to be wirelessly connected to said network and to communicate with said wired network through communications encrypted with an encryption key, said wireless station comprising:

a wireless network communications device containing said encryption key, said wireless station configured to access said encryption key on said wireless network communications device during said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to said wired encryption key updating device wired to said network to receive, store, and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device.

9. (Previously Presented) A wireless network as in claim 8, wherein said new encryption key is a randomly generated encryption key.

10. (Original) A wireless network as in claim 8, wherein said new encryption key is generated by said generator and transmitted by said wired network communications device at user-defined intervals.

11. (Original) A wireless network as in claim 8, wherein when a newly generated encryption key is the same as one of k previously used encryption keys, said encryption key generator generates a new encryption key.

12. (Original) A wireless network as in claim 11, wherein k is a user-defined number.

13. (Cancelled)

14. (Previously Presented) A wireless network as in claim 8, further comprising a card tray at said updating device, said wireless network communications device being connected to said wired network by insertion of said wireless network communications device into said card tray.

15. (Previously Presented) A wireless network station comprising:

a wireless network communications device for conducting wireless communications with a wired network, said wireless network communications device being physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable to a wired network to receive, store, and use a new encryption key, said wireless station configured to access an encryption key on said wireless network communications device during a wireless communication.

16. (Previously Presented) A wireless station as in claim 15, wherein said wireless network communications device is adapted to be physically connected to a wired network by being insertable into a card tray physically connected to said wired network.

17. (Previously Presented) A wireless network communications device comprising:

a removable wireless communications network card adapted to be physically connected to and disconnected from a wireless station card interface; and

a storage area on said network card which stores an updateable encryption key for use by a wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface which supplies a new encryption key, said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication.

18. (Previously Presented) A wireless network communications card as in claim 17, wherein said card interface for providing a new encryption key is a PCMCIA card interface.

19. (Previously Presented) A wireless network communications card as in claim 18, wherein said PCMCIA card interface is provided at a PCMCIA card tray.

20. (Previously Presented) An encryption key programming system comprising:

an encryption key generator connected to a wired network; and

a programming device connected to said wired network for receiving over a wire connection a new encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updateable encryption key and storing said received encryption key in said wireless network communications device, said

new encryption key on said wireless network communications device being accessible by a wireless network device during encrypted communications.

21. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a random encryption key.

22. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key at user-defined intervals.

23. (Original) An encryption key programming system as in claim 20, wherein said encryption key generator generates a new encryption key on user-specified days.

24. (Previously Presented) An encryption key programming system as in claim 20, wherein said encryption key generator generates a first new encryption key, compares said new encryption key to the previous k encryption keys used in said network and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

25. (Original) An encryption key programming system as in claim 20, wherein k is a user-defined number of previously used encryption keys.

26. (Original) An encryption key programming system as in claim 20, further comprising a card tray connected to said programming device, said wireless communications device being received by said programming device by insertion of said wireless communications device into said card tray.

APPENDIX B – EVIDENCE APPENDIX
NONE

APPENDIX C – RELATED PROCEEDINGS APPENDIX
NONE